Red Hat Network Satellite 5.5 Proxy Installation Guide

Red Hat Network Satellite
Edition 3

Landmann

Red Hat Network Satellite 5.5 Proxy Installation Guide

Red Hat Network Satellite
Edition 3

Landmann
rlandmann@redhat.com

Legal Notice

Copyright © 2010 Red Hat, Inc.

This document is licensed by Red Hat under the Creative Commons Attribution-ShareAlike 3.0 Unported License. If you distribute this document, or a modified version of it, you must provide attribution to Red Hat, Inc. and provide a link to the original. If the document is modified, all Red Hat trademarks must be removed.

Red Hat, as the licensor of this document, waives the right to enforce, and agrees not to assert, Section 4d of CC-BY-SA to the fullest extent permitted by applicable law.

Red Hat, Red Hat Enterprise Linux, the Shadowman logo, JBoss, MetaMatrix, Fedora, the Infinity Logo, and RHCE are trademarks of Red Hat, Inc., registered in the United States and other countries.

Linux ® is the registered trademark of Linus Torvalds in the United States and other countries.

Java ® is a registered trademark of Oracle and/or its affiliates.

XFS ® is a trademark of Silicon Graphics International Corp. or its subsidiaries in the United States and/or other countries.

MySQL ® is a registered trademark of MySQL AB in the United States, the European Union and other countries.

Node.js ® is an official trademark of Joyent. Red Hat Software Collections is not formally related to or endorsed by the official Joyent Node.js open source or commercial project.

The OpenStack ® Word Mark and OpenStack Logo are either registered trademarks/service marks or trademarks/service marks of the OpenStack Foundation, in the United States and other countries and are used with the OpenStack Foundation's permission. We are not affiliated with, endorsed or sponsored by the OpenStack Foundation, or the OpenStack community.

All other trademarks are the property of their respective owners.

Abstract

Welcome to the RHN Proxy Installation Guide.

Table of Contents

Chapter 1. Introduction **4**
1.1. Red Hat Network 4
1.2. Frequently Used Terminologies 4
1.3. RHN Proxy Server 5
1.4. How Proxy Works 6

Chapter 2. Requirements **8**
2.1. Software Requirements 8
2.2. Hardware Requirements 9
2.3. Disk Space Requirements 9
2.4. Additional Requirements 9

Chapter 3. Example Topologies **12**
3.1. Single Proxy Topology 12
3.2. Multiple Proxy Horizontally Tiered Topology 12
3.3. Multiple Proxy Vertically Tiered Topology 13
3.4. Proxies with RHN Satellite Server 14

Chapter 4. Installation **15**
4.1. Base Install 15
4.2. RHN Proxy Server Installation Process 15
4.2.1. The Answer File 18

Chapter 5. RHN Package Manager and Serving Local Packages **20**
5.1. Creating a Private Channel 22
5.2. Uploading Packages 22

Chapter 6. Upgrade Installation **24**
6.1. Pre-Requisites 24
6.2. Upgrade Installation Process 24

Chapter 7. Troubleshooting **25**
7.1. Managing the Proxy Service 25
7.2. Log Files 25
7.3. Questions and Answers 25
7.4. General Problems 26
7.5. Host Not Found/Could Not Determine FQDN 27
7.6. Connection Errors 27
7.7. Caching Issues 28
7.8. Proxy Debugging by Red Hat 29

Sample RHN Proxy Server Configuration File **30**

Revision History **31**

Index **31**
A 31
C 32
D 32
F 32
G 32
H 32
I 32
L 33

O 33
P 33
Q 33
R 33
S 34
T 34

Chapter 1. Introduction

1.1. Red Hat Network

Red Hat Network (RHN) is the environment for system-level support and management of Red Hat systems and networks of systems. Red Hat Network brings together the tools, services, and information repositories needed to maximize the reliability, security, and performance of their systems. To use RHN, system administrators register the client system's System Profiles, which contain the software and hardware profiles of the system, with Red Hat Network. When a client system requests package updates, only the applicable packages for the client are returned (based upon the software profile stored on the RHN Servers).

Advantages of using Red Hat Network include:

- Scalability — with Red Hat Network, a single system administrator can set up and maintain hundreds or thousands of Red Hat systems more easily, accurately, and quickly than they could maintain a single system without Red Hat Network.
- Standard Protocols — standard protocols are used to maintain security and increase capability. For example, XML-RPC gives Red Hat Network the ability to do much more than merely download files.
- Security — all communication between registered systems and Red Hat Network takes place over secure Internet connections.
- View Errata Alerts — easily view Errata Alerts for all your client systems through one website.
- Scheduled Actions — use the website to schedule actions, including Errata Updates, package installs, and software profile updates.
- Simplification — maintaining Red Hat systems becomes a simple, automated process.

1.2. Frequently Used Terminologies

Before understanding RHN Proxy Server, it is important to become familiar with the following Red Hat Network terms:

Channel

A channel is a list of software packages. There are two types of channels: base channels and child channels. A *base channel* consists of a list of packages based on a specific architecture and Red Hat release. A *child channel* is a channel associated with a base channel that contains extra packages.

Organization Administrator

An Organization Administrator is a user role with the highest level of control over an organization's Red Hat Network account. Members with this role can add other users, other systems, and system groups to the organization, as well as remove them. A Red Hat Network organization is required to have at least one Organization Administrator.

Channel Administrator

A Channel Administrator is a user role with full access to channel management capabilities. Users with this role are capable of creating channels and assigning packages to channels. This role can be assigned by an Organization Administrator through the **Users** tab of the RHN website.

Red Hat Update Agent

The Red Hat Update Agent is the Red Hat Network client application (**up2date** or **yum**) that allows users to retrieve and install new or updated packages for the client system on which the application is run.

Traceback

A traceback is a detailed description of "what went wrong" that is useful for troubleshooting the RHN Proxy Server. Tracebacks are automatically generated when a critical error occurs and are emailed to the individual(s) designated in the RHN Proxy Server's configuration file.

For more detailed explanations of these terms and others, refer to the *Red Hat Network Reference Guide* available at http://www.redhat.com/docs/manuals/satellite/ and the **Help** page on the Satellite Web user interface.

1.3. RHN Proxy Server

A RHN Proxy Server is a package-caching mechanism that reduces the bandwidth requirements for RHN and enables custom package deployment. Proxy customers cache RPMs, such as Errata Updates from Red Hat or custom RPMs generated by their organization, on an internal, centrally-located server. Client systems then receive these updates from the Proxy rather than by accessing the Internet individually.

Although the packages are served by the Proxy, clients' System Profiles and user information are stored on the secure, central RHN Servers [1], which also serve the RHN website (rhn.redhat.com). The Proxy acts as a go-between for client systems and Red Hat Network (or an RHN Satellite Server). Only the package files are stored on the RHN Proxy Server. Every transaction is authenticated, and the Red Hat Update Agent checks the GPG signature of each package retrieved from the local RHN Proxy Server.

In addition to storing official Red Hat packages, the RHN Proxy Server can be configured to deliver an organization's own custom packages from private RHN *channels*, using the RHN Package Manager. For instance, an organization could develop its own software, package it in an RPM, sign it with its own GPG signature, and have the local RHN Proxy Server update all of the individual systems in the network with the latest versions of the custom software.

Advantages of using RHN Proxy Server include:

- Scalability — there can be multiple local RHN Proxy Servers within one organization.
- Security — an end-to-end secure connection is maintained: from the client systems, to the local RHN Proxy Server, to the Red Hat Network servers.
- Saves time — packages are delivered significantly faster over a local area network than the Internet.
- Saves bandwidth — packages are downloaded from RHN only once (per local Proxy Server's caching mechanism) instead of downloading each package to each client system.
- Customized updates — create a truly automated package delivery system for custom software packages, as well as official Red Hat packages required for the client systems. Custom private RHN channels allow an organization to automate delivery of in-house packages.
- Customized configuration — restrict or grant updates to specific architectures and OS versions.
- Only one Internet connection required — Because clients connect only to the RHN Proxy Server and not the Internet, they require only a Local Area Network connection to the Proxy. Only the RHN Proxy Server needs an Internet connection to contact the RHN Servers, unless the RHN Proxy Server is using a RHN Satellite Server, in which case only the RHN Satellite Server requires an Internet connection.

1.4. How Proxy Works

The Red Hat Update Agent or **Package Updater** on the client systems does not directly contact a Red Hat Network Server. Instead, the client (or clients) connects in turn to an RHN Proxy Server that connects to the Red Hat Network Servers or to a RHN Satellite Server. Thus, the client systems do not need direct access to the Internet. They need access only to the RHN Proxy Server.

Important

Red Hat strongly recommends that clients connected to an RHN Proxy Server be running the latest update of Red Hat Enterprise Linux to ensure proper connectivity.

Clients that access RHN directly are authenticated by the RHN servers. Clients that access an RHN Proxy Server are still authenticated by RHN; however, in this case the Proxy provides both authentication and route information to RHN. After a successful authentication, the Red Hat Network Server informs the RHN Proxy Server that it is permitted to execute a specific action for the client. The RHN Proxy Server downloads all of the updated packages (if they are not already present in its cache) and delivers them to the client system.

Requests from the Red Hat Update Agent or Package Updater on the client systems are still authenticated on the server side, but package delivery is significantly faster since the packages are cached in the HTTP Proxy Caching Server; or the RHN Proxy Server (for local packages); the RHN Proxy Server and client system are connected via the LAN and are limited only by the speed of the local network.

Authentication is done in the following order:

1. The client performs a login action at the beginning of a client session. This login is passed through one or more RHN Proxy Servers until it reaches a Red Hat Network Server.
2. The Red Hat Network Server attempts to authenticate the client. If authentication is successful, the server then passes back a session token via the chain of RHN Proxy Servers. This token, which has a signature and expiration, contains user information, including channel subscriptions, username, etc.
3. Each RHN Proxy Server caches this token on its local file system in **/var/cache/rhn/**. Caching reduces some of the overhead of authenticating with Red Hat Network Servers and greatly improves the performance of Red Hat Network.
4. This session token is passed back to the client machine and is used in subsequent actions on Red Hat Network.

From the client's point of view, there is no difference between an RHN Proxy Server and a Red Hat Network Server. From the Red Hat Network Server's point of view, an RHN Proxy Server is a special type of RHN client. Clients are thus not affected by the route a request takes to reach a Red Hat Network Server. All the logic is implemented in the RHN Proxy Servers and Red Hat Network Servers.

Optionally, the RHN Package Manager can be installed and configured to serve custom packages. Any package that is not an official Red Hat package, including custom packages written specifically for an organization, can only be served from a private software channel (also referred to as a custom software channel). After creating a private RHN channel, the custom RPM packages are associated with that channel by uploading the package headers to the RHN Servers. Only the headers are uploaded, not the actual package files. The headers are required because they contain crucial RPM information, such as software dependencies, that allows RHN to automate package installation. The actual custom RPM

packages are stored on the RHN Proxy Server and sent to the client systems from inside the organization's local area network.

Configuring a computer network to use RHN Proxy Servers is straightforward. The Red Hat Network applications on the client systems must be configured to connect to the RHN Proxy Server instead of the Red Hat Network Servers. Refer to the *RHN Client Configuration Guide* for details. On the proxy side, one has to specify the next proxy in the chain (which eventually ends with a Red Hat Network Server). If the RHN Package Manager is used, the client systems must be subscribed to the private RHN channel.

[1] Throughout this document, "RHN" may refer to either RHN's Hosted site (http://rhn.redhat.com) or an RHN Satellite Server.

Chapter 2. Requirements

This chapter focuses on the requirements that need to be met before you can install RHN Proxy Server. Remember that the Satellite must be a version greater than or equal to the version of the Proxy that is being installed. For example, to install RHN Proxy Server 5.4, the Satellite version should be 5.4 or later, and can not be 5.3 or lower.

2.1. Software Requirements

To perform an installation, the following software-related components must be available:

- Base operating system — RHN Proxy Server is supported with Red Hat Enterprise Linux 5 and 6. The operating system can be installed from disc, local ISO image, kickstart, or any of the methods supported by Red Hat.

  RHN Proxy Server can be installed on Red Hat Enterprise Linux 5 and 6 in any virtualized environment supported by Red Hat, including Xen, KVM, and VMware.

  Note that for production deployments, it is recommended to deploy RHN Proxy Server as the sole application running on the underlying physical hardware to avoid contention issues. Also, be aware that functional support for virtualized environments does not always equal the performance of running on physical hardware, so carefully consider the virtualized environment of choice and any tuning guidelines recommended.

  Note

  Each purchased RHN Proxy product includes one supported instance of Red Hat Enterprise Linux Server. RHN Proxy must be installed onto a fresh installation of Enterprise Linux where RHN Proxy is the only application and service provided by the OS. Using the Red Hat Enterprise Linux OS included in RHN Proxy to run other daemons, applications, or services within the environment is not supported.

  Each version of Red Hat Enterprise Linux requires a certain package set to support RHN Proxy Server . Adding more packages can cause errors during installation. Therefore, Red Hat recommends obtaining the desired package set in the following ways:

  Note

  For kickstarting, specify the following package group: **`@Base`**
  For installing Red Hat Enterprise Linux via CD or ISO image, select the following package group: **`Minimal`**

- An available RHN Proxy Server entitlement within the RHN Satellite Server account.
- An available Provisioning entitlement within the RHN Satellite Server account (which should come packaged with the RHN Proxy Server entitlement).
- Access to the Red Hat Network Tools channel for the installed version of Red Hat Enterprise Linux. This channel includes the **`spacewalk-proxy-installer`** package that contains the **`configure-proxy.sh`** installation program required to install RHN Proxy Server .
- All **`rhncfg*`** packages installed on the Proxy (from the RHN Tools channel).
- Either the **`spacewalk-certs-tools`** package installed on the Proxy (from the RHN Tools channel) for RHN Hosted users, or the secure sockets layer (SSL) CA certificate password used to generate the parent server certificate for RHN Satellite Server users.

- Configuration of the system to accept remote commands and configuration management through Red Hat Network if using the deprecated Web UI installation method. Refer to Section 4.2, “RHN Proxy Server Installation Process” for instructions.

2.2. Hardware Requirements

The following hardware configuration is required for the RHN Proxy Server :

- A Pentium IV Processor or equivalent
- 512 MB of memory
- At least 5 GB storage for base install of Red Hat Enterprise Linux
- 6 GB storage per distribution/channel

The load on the Apache Web server is directly related to the frequency with which client systems connect to the Proxy. If the default interval of four hours (or 240 minutes) as set in the **/etc/sysconfig/rhn/rhnsd** configuration file of the client systems is reduced, the load on this component *increases* significantly.

2.3. Disk Space Requirements

The caching mechanism used by RHN Proxy Server is the Squid HTTP proxy, which saves significant bandwidth for the clients. It should have a reasonable amount of space available. The cached packages are stored in **/var/spool/squid**. The required free space allotment is 6 GB storage per distribution/channel.

If the RHN Proxy Server is configured to distribute custom, or local packages, make sure that the **/var** mount point on the system storing local packages has sufficient disk space to hold all of the custom packages, which are stored in **/var/spool/rhn-proxy**. The required disk space for local packages depends on the number of custom packages served.

2.4. Additional Requirements

The following additional requirements must be met before the RHN Proxy Server installation can be considered complete:

Full Access

Client systems need full network access to the RHN Proxy Server services and ports.

Firewall Rules

RHN strongly recommends firewalling the RHN Proxy Server solution from the Internet. However, various TCP ports must be opened on the Proxy, depending on your implementation of RHN Proxy Server :

Table 2.1. Ports to open on the Proxy

Port	Direction	Reason
80	Outbound	Proxy uses this port to reach rhn.redhat.com, xmlrpc.rhn.redhat.com, and your Satellite URL (depending on whether RHN Proxy is talking to either RHN Hosted or a Satellite Server).
80	Inbound	Client requests come in via either http or https
443	Inbound	Client requests come in via either http or https
443	Outbound	Proxy uses this port to reach rhn.redhat.com, xmlrpc.rhn.redhat.com, and the Satellite URL (depending on whether RHN Proxy is talking to either RHN Hosted or a Satellite Server).
4545	Outbound	If your Proxy is connected to an RHN Satellite Server, Monitoring makes connections to **rhnmd** running on client systems via this TCP port, if Monitoring is enabled and probes configured to registered systems.
5222	Inbound	Opening this port allows **osad** client connections to the **jabberd** daemon on the Proxy when using RHN Push technology.
5269	Outbound	If the Proxy is connected an RHN Satellite Server, this port must be open to allows server-to-server connections via **jabberd** for RHN Push Technology.

Synchronized System Times

There is great time sensitivity when connecting to a Web server running SSL (Secure Sockets Layer); it is imperative the time settings on the clients and server are reasonably close together so that the SSL certificate does not expire before or during use. It is recommended that Network Time Protocol (NTP) be used to synchronize the clocks.

Fully Qualified Domain Name (FQDN)

The system upon which the RHN Proxy Server will be installed must resolve its own FQDN properly.

A Red Hat Network Account

Customers who will be connecting to the central Red Hat Network Servers to receive incremental updates must have a Red Hat Network account. The sales representative assists with the setup of this account at the time of purchase.

Backups of Login Information

It is imperative that customers keep track of all primary login information. For RHN Proxy Server , this includes usernames and passwords for the Organization Administrator account and SSL certificate generation. Red Hat strongly recommends this information be copied onto two separate back-up disks (CD/DVD/removable hard drives), printed out on paper, and stored in a safe place.

Distribution Locations

Since the Proxy forwards virtually all local HTTP requests to the central RHN Servers, take care in putting files destined for distribution (such as in a kickstart installation tree) in the non-forwarding location on the Proxy: **`/var/www/html/pub/`**. Files placed in this directory can be downloaded directly from the Proxy. This can be especially useful for distributing GPG keys or establishing installation trees for kickstarts.

In addition, Red Hat recommends that the system running the code should not be publicly available. No users but the system administrators should have shell access to these machines. All unnecessary services should be disabled. Use **`ntsysv`** or **`chkconfig`** to disable services.

Finally, have the following technical documents in hand for use in roughly this order:

1. *The RHN Proxy Server Installation Guide* — This guide, which you are now reading, provides the essential steps necessary to get an RHN Proxy Server up and running.
2. *The RHN Client Configuration Guide* — This guide explains how to configure the systems to be served by an RHN Proxy Server or RHN Satellite Server. (This will also likely require referencing *The RHN Reference Guide*, which contains steps for registering and updating systems.)
3. *The RHN Channel Management Guide* — This guide identifies in great detail the recommended methods for building custom packages, creating custom channels, and managing private Errata.
4. *The RHN Reference Guide* — This guide describes how to create RHN accounts, register and update systems, and use the RHN website to its utmost potential. This guide will probably come in handy throughout the installation and configuration process.

Chapter 3. Example Topologies

The RHN Proxy Server can be configured in multiple ways. Select one method depending on the following factors:

1. The total number of client systems to be served by the RHN Proxy Server
2. The maximum number of clients expected to connect *concurrently* to the RHN Proxy Server.
3. The number of custom packages and channels to be served by the RHN Proxy Server.
4. The number of RHN Proxy Servers being used in the customer environment.

The rest of this chapter describes possible configurations and explains their benefits.

3.1. Single Proxy Topology

The simplest configuration is to use a single RHN Proxy Server to serve the entire network. This configuration is adequate to service a small group of clients and a network that would benefit from caching Red Hat RPMs and storing custom packages on a local server.

The disadvantage of using one RHN Proxy Server is that performance will be compromised as the number of clients requesting packages grows.

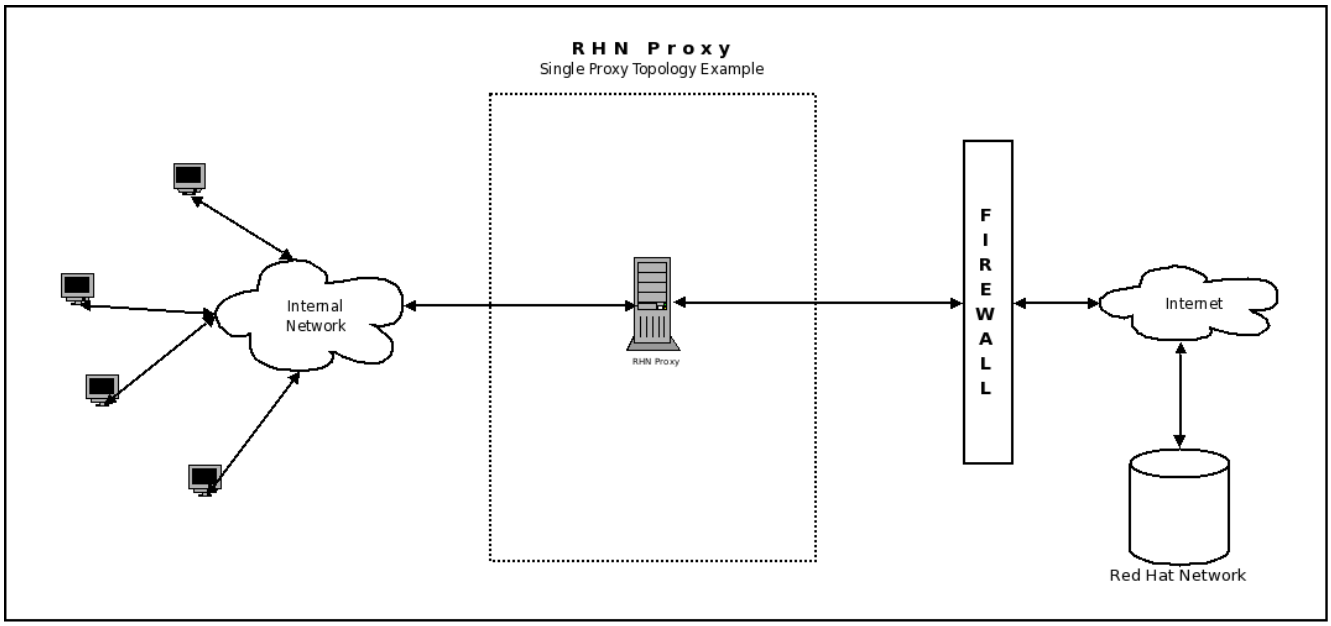

Figure 3.1. Single Proxy Topology

3.2. Multiple Proxy Horizontally Tiered Topology

For larger networks, a more distributed method may be needed, such as having multiple RHN Proxy Servers all connecting to Red Hat Network individually. This horizontally tiered configuration balances the load of client requests while enabling each Proxy to simultaneously synchronize with RHN.

A disadvantage of this horizontal structure is that custom packages loaded to an individual Proxy must be distributed to its sibling servers. This situation can be addressed in one of two ways:

- The **rsync** file transfer program can be used to synchronize packages between the Proxies
- A Network File System (NFS) share can be established between the Proxies and the custom channel

repository.

Either of these solutions will allow any client of any RHN Proxy Servers to have all custom packages delivered to them.

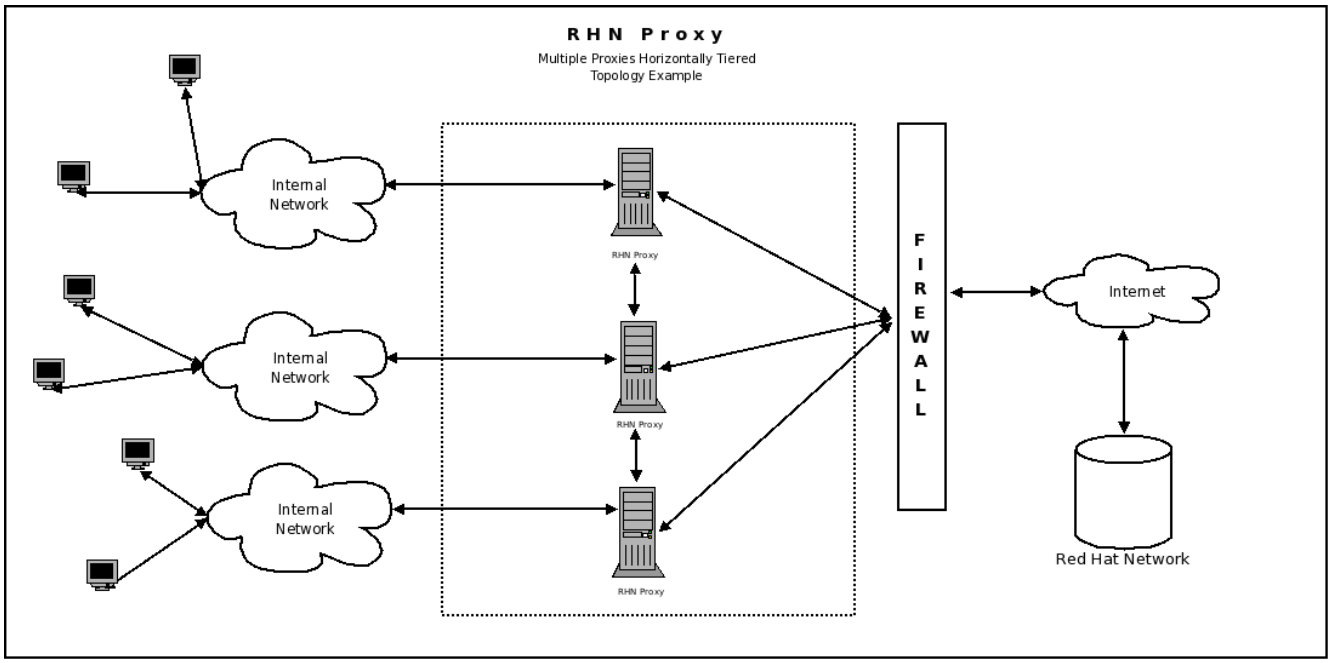

Figure 3.2. Multiple Proxy Horizontally Tiered Topology

3.3. Multiple Proxy Vertically Tiered Topology

An alternative method for multiple RHN Proxy Servers is to establish a primary Proxy that the others connect to for RPMs from Red Hat Network and custom packages created locally. In essence, the secondary Proxies act as clients of the primary. This alleviates the need to establish synchronization between the RHN Proxy Servers as they use the **`up2date`** functionality inherent with the product.

Like the horizontally tiered configuration, this vertical method allows any client of any RHN Proxy Servers to have all custom packages delivered to them. The Proxy merely looks in its repository to see if it can find the package on its file system. If not, it then makes the attempt from the next level up.

This vertically tiered configuration ensures that the secondary Proxies depend upon the primary for updates from RHN, as well as for custom packages. Also, custom channels and packages must be placed on the primary Proxy only, to ensure distribution to the child Proxies. Finally, the configuration files of the secondary Proxies must point to the primary, instead of directly at Red Hat Network.

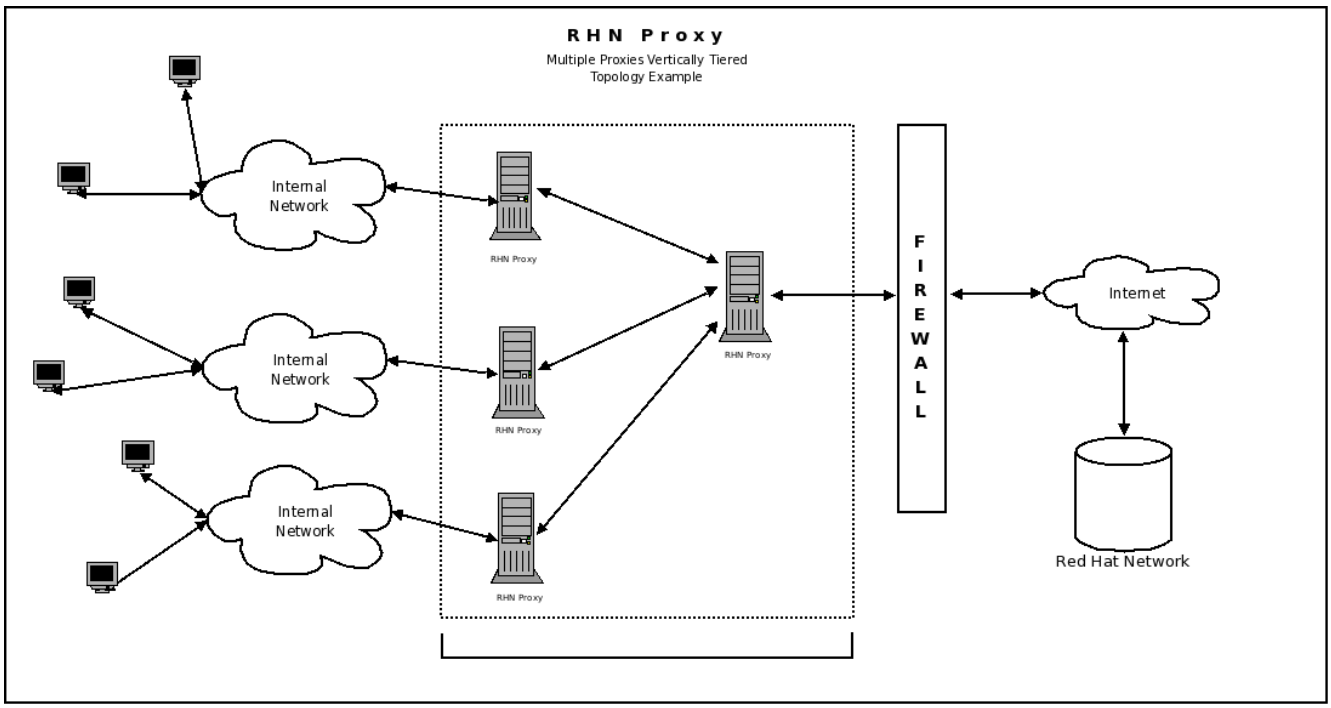

Figure 3.3. Multiple Proxy Vertically Tiered Topology

3.4. Proxies with RHN Satellite Server

In addition to the methods described in detail within this chapter, customers also have the option of using RHN Proxy Server in conjunction with RHN Satellite Server. This works similarly to the vertically tiered Proxy configuration but increases capacity significantly, as Satellites can serve a much greater number of client systems.

For a thorough description of this combination, refer to the Example Topologies chapter of the *RHN Satellite Server Installation Guide*. Linking the two products' SSL certificates is described in the *RHN Client Configuration Guide*. To find out how channels and packages are shared between them, refer to the *RHN Channel Management Guide*.

Chapter 4. Installation

This chapter describes the initial installation of the RHN Proxy Server. It presumes the prerequisites listed in Chapter 2, *Requirements* have been met. However, if you are *upgrading* to a newer version of RHN Proxy Server, contact your Red Hat representative for assistance.

4.1. Base Install

The RHN Proxy Server is designed to run on the Red Hat Enterprise Linux operating system. Therefore, the first phase is to install the base operating system, either from disc, ISO image, or kickstart. During and after operating system installation, make sure you:

- Allocate sufficient space to the partition that will be used to store packages, according to the hardware requirements set forth earlier. The default location for cached Red Hat packages is **/var/spool/squid**, while custom packages are located in **/var/spool/rhn-proxy**.

  Note

  The installation program automatically calculates the available space on the partition where **/var/spool/squid** is mounted and allocates up to 60 percent of the free space for RHN Proxy Server use.

- Install the packages required by RHN Proxy Server.

  Important

  Install only the base packages, as others will cause the RHN Proxy Server installation to fail.

  Refer to Section 2.1, “Software Requirements” for the method to obtain the correct package group needed for each version of Red Hat Enterprise Linux.
- Enable Network Time Protocol (NTP) on the Proxy and select the appropriate time zone. All client systems should already be running the **ntpd** daemon and be set to the correct time zone.
- Disable the **ipchains** and **iptables** services after installation.

4.2. RHN Proxy Server Installation Process

The following instructions describe the RHN Proxy Server installation process:

1. Log in as the root user on the intended RHN Proxy Server system.
2. Register the newly-installed Red Hat Enterprise Linux system with Red Hat Network (either the central RHN Servers or on the RHN Satellite Server) using the organizational account containing the RHN Proxy Server entitlement with the command: **rhn_register**.
3. Subscribe the client to the RHN Tools channel.
4. Install the proxy installer:

   ```
   yum install spacewalk-proxy-installer
   ```

5. Perform the installation:

   ```
   configure-proxy.sh
   ```

Note

In order to perform this step successfully, root access to the Satellite server is required. Alternatively, add the **--force-own-ca** option to the command.

The command-line installation program leads users through a series of prompts regarding RHN Proxy Server installation and initial configuration details such as installation options and SSL certificate generation. The following instructions describe the installation process:

Tip

If you press **Enter** at a prompt instead of typing in an entry, the RHN Proxy Server command-line installation program uses the default response enclosed in brackets. Alternatively, if you want to use default answers without *any* user interaction, use the **--non-interactive** option, which will use all default responses.

6. The first series of prompts are site-specific details about the installation.

```
Proxy version to activate [5.4]:
```

The **Proxy version** prompts for confirmation on the version of RHN Proxy Server to install.

```
RHN Parent [satserver.example.com]:
```

The **RHN Parent** is the domain name or address of the system that serves the Proxy, which could be the RHN Hosted servers (xmlrpc.rhn.redhat.com), or a Satellite server.

```
Traceback email []:
```

The **Traceback email** is the email address to which error-related traceback messages are mailed, usually the email of the Proxy administrator. Use commas to separate more than one email address at this prompt.

7. The next series of prompts are related to configuring the details for generating an SSL certificate, which is recommended to secure traffic to and from the RHN Proxy Server.

```
Use SSL [Y/n]: y
```

In the **Use SSL** prompt, type **y** to configure the RHN Proxy Server to support SSL.

```
CA Chain [/usr/share/rhn/RHN-ORG-TRUSTED-SSL-CERT]:
```

In the **CA Chain** prompt, press **Enter** to use the default path for the Certificate Authority (CA) Chain, which if the RHN Proxy is communicating with an RHN Satellite then this value is usually **/usr/share/rhn/RHN-ORG-TRUSTED-SSL-CERT**. If it is communicating with RHN Hosted, it is usually the **/usr/share/rhn/RHNS-CA-CERT** file. Custom SSL certificates must be located in the **/usr/share/rhn/** directory.

```
HTTP Proxy []:
```

If the RHN Proxy Server connects through an HTTP proxy, enter the proxy hostname and port number, such as **`corporate.proxy.example.com:3128`**

Enter the required details necessary to generate a proper SSL server certificate, including the **`Organzation`** name, the **`Organization Unit`** (such as **`Engineering`**), the **`Common Name`** (the domain name), as well as the details for City, State and Country. Finally, enter the email address for the administrator or technical contact in charge of SSL certificates.

```
Regardless of whether you enabled SSL for the connection to the Proxy Parent
Server, you will be prompted to generate an SSL certificate.
This SSL certificate will allow client systems to connect to this Spacewalk
Proxy
securely. Refer to the Spacewalk Proxy Installation Guide for more
information.
Organization: Example Company
Organization Unit [proxy1.example.com]:
Common Name: proxy1.example.com
City: New York
State: New York
Country code: US
Email [admin@example.com]:
```

8. As a result of running the RHN Proxy Server installation program, the command-line installation program:
   - Prompts for the installation of monitoring support to RHN Proxy Server.
   - Allows the organization to create and populate a configuration channel for future RHN Proxy Server installations.
   - Finalizes SSL configuration.
   - Restarts any service daemons that had modified configurations.

```
You do not have monitoring installed. Do you want to install it?
Will run 'yum install spacewalk-proxy-monitoring'.  [Y/n]:n
```

Confirm whether or not you want to install Monitoring support on the Proxy server.

```
Generating CA key and public certificate:
CA password:
CA password confirmation:
Copying CA public certificate to /var/www/html/pub for distribution to
clients:
Generating SSL key and public certificate:
CA password:
Backup made: 'rhn-ca-openssl.cnf' --> 'rhn-ca-openssl.cnf.1'
Rotated: rhn-ca-openssl.cnf --> rhn-ca-openssl.cnf.1
Installing SSL certificate for Apache and Jabberd:
Preparing packages for installation...
rhn-org-httpd-ssl-key-pair-proxy1.example-1.0-1
```

The **`configure-proxy.sh`** program then configures SSL, prompting you to create a Certificate Authority password and confirm it before generating the SSL keys and the public certificate.

```
Create and populate configuration channel rhn_proxy_config_1000010000? [Y]:
Using server name satserver.example.com
Red Hat Network username: admin
Password:
Creating config channel rhn_proxy_config_1000010000
Config channel rhn_proxy_config_1000010000 created
using server name satserver.example.com
Pushing to channel rhn_proxy_config_1000010000:
Local file /etc/httpd/conf.d/ssl.conf -> remote file
/etc/httpd/conf.d/ssl.conf
Local file /etc/rhn/rhn.conf -> remote file /etc/rhn/rhn.conf
Local file /etc/rhn/cluster.ini -> remote file /etc/rhn/cluster.ini
Local file /etc/squid/squid.conf -> remote file /etc/squid/squid.conf
Local file /etc/httpd/conf.d/cobbler-proxy.conf -> remote file
/etc/httpd/conf.d/cobbler-proxy.conf
Local file /etc/httpd/conf.d/rhn_proxy.conf -> remote file
/etc/httpd/conf.d/rhn_proxy.conf
Local file /etc/httpd/conf.d/rhn_broker.conf -> remote file
/etc/httpd/conf.d/rhn_broker.conf
Local file /etc/httpd/conf.d/rhn_redirect.conf -> remote file
/etc/httpd/conf.d/rhn_redirect.conf
Local file /etc/jabberd/c2s.xml -> remote file /etc/jabberd/c2s.xml
Local file /etc/jabberd/sm.xml -> remote file /etc/jabberd/sm.xml
```

The installer then asks whether or not you wish to create a configuration channel based on the configuration files created while running **`configure-proxy.sh`**. The installer will then create a RHN Satellite Server configuration channel based on the name of the client system upon which RHN Proxy Server is installed (in the example above the sysID is 1000010000), and collects the various **`httpd`**, SSL, **`squid`**, and **`jabberd`** server files that will comprise the configuration channel for the Proxy server.

9. Finally, the installer starts and restarts all RHN Proxy Server related services and exits when completed.

```
Enabling Satellite Proxy
Shutting down rhn-proxy...
Shutting down Jabber router:                               [  OK  ]
Stopping httpd:                                            [  OK  ]
Stopping squid:                                            [  OK  ]
Done.
Starting rhn-proxy...
init_cache_dir /var/spool/squid... Starting squid: .       [  OK  ]
Starting httpd:                                            [  OK  ]
Starting Jabber services                                   [  OK  ]
Done.
```

4.2.1. The Answer File

To automate some of the process of installing RHN Proxy Server on your systems, the **`configure-proxy.sh`** program allows administrators to create *answer files* that contain pre-filled responses to prompts in the installation program.

The following is an example answer file that contains pre-filled answers related to version number, the RHN Satellite Server server that serves as the parent server, SSL, and other configuration parameters. For more information about creating and using answer files, refer to the **`configure-proxy.sh`** manual page by typing **`man configure-proxy.sh`** at a shell prompt.

```
# example of answer file for configure-proxy.sh
# for full list of possible option see
# man configure-proxy.sh

VERSION=5.4
RHN_PARENT=rhn-satellite.example.com
TRACEBACK_EMAIL=jsmith@example.com
USE_SSL=1
SSL_ORG="Red Hat"
SSL_ORGUNIT="Spacewalk"
SSL_CITY=Raleigh
SSL_STATE=NC
SSL_COUNTRY=US
INSTALL_MONITORING=N
ENABLE_SCOUT=N
CA_CHAIN=/usr/share/rhn/RHN-ORG-TRUSTED-SSL-CERT
POPULATE_CONFIG_CHANNEL=Y
```

To use an answer file (called **`answers.txt`** for example) with **`configure-proxy.sh`**, type the following:

```
configure-proxy.sh --answer-file=answers.txt
```

Chapter 5. RHN Package Manager and Serving Local Packages

The RHN Package Manager is a command line tool that allows an organization to serve local packages associated with a private RHN channel through the RHN Proxy Server. To update only official Red Hat packages for the RHN Proxy Server, do not install the RHN Package Manager.

To use the RHN Package Manager, install the **`spacewalk-proxy-package-manager`** package and its dependencies.

Only the header information for packages is uploaded to the RHN Servers. The headers are required so that RHN can resolve package dependencies for the client systems. The actual package files (**`*.rpm`**) are stored on the RHN Proxy Server.

The RHN Package Manager uses the same settings as the Proxy, defined in the **`/etc/rhn/rhn.conf`** configuration file.

Here is a summary of all the command line options for RHN Package Manager **`rhn_package_manager`**:

Table 5.1. `rhn_package_manager` options

Option	Description
-v, **--verbose**	Increase verbosity.
-d*DIR*, **--dir=*DIR***	Process packages from directory ***DIR***.
-c*CHANNEL*, **--channel=*CHANNEL***	Manage this channel — may be present multiple times.
-n*NUMBER*, **--count=*NUMBER***	Process this number of headers per call — the default is 32.
-l, **--list**	List each package name, version number, release number, and architecture in the specified channel(s).
-s, **--sync**	Check if local directory is in sync with the server.
-p, **--printconf**	Print the current configuration and exit.
-X*PATTERN*, **--exclude=*PATTERN***	Exclude files matching this glob expression — can be present multiple times.
--newest	Push only the packages that are newer than packages already pushed to the server for the specified channel.
--stdin	Read the package names from stdin.
--nosig	Push unsigned packages. By default the RHN Package Manager attempts to push only signed packages.
--username=*USERNAME*	Specify your RHN username. If you do not provide one with this option, you will be prompted for it.
--password=*PASSWORD*	Specify your RHN password. If you do not provide one with this option, you will be prompted for it.
--source	Upload source package headers.
--dontcopy	In the post-upload step, do not copy the packages to their final location in the package tree.
--test	Only print the packages to be pushed.
--no-ssl	*Not recommended* — Turn off SSL.
-?, **--usage**	Briefly describe the options.
--copyonly	Copies the file listed in the argument into the specified channel. Useful when a channel on the proxy is missing a package and you don't want to reimport all of the packages in the channel. E.g., **`rhn_package_manager -c`*CHANNEL*`--copyonly`*/PATH/TO/MISSING/FILE***
-h, **--help**	Display the help screen with a list of options.

Tip

These command line options are also described in the **`rhn_package_manager`** man page: **`man rhn_package_manager`**.

In order for RHN Package Manager to be able to serve the local packages, the following steps need to be followed:

1. Create a private channel.
2. Upload the local packages into the channel.

The steps will be further discussed in the next sections.

5.1. Creating a Private Channel

Before local packages can be provided through the RHN Proxy Server, a private channel is needed to store them. Perform the following steps to create a private channel:

1. Log in to the RHN Web interface at https://rhn.redhat.com.
2. Click **Channels** on the top navigation bar. If the **Manage Channels** option is not present in the left navigation bar, ensure that this user has channel editing permissions set. Do this through the **Users** category accessible through the top navigation bar.
3. In the left navigation bar, click **Manage Software Channels** and then the **create new channel** button at the top-right corner of the page.
4. Select a parent channel and base channel architecture, then enter a name, label, summary, and description for the new private channel. The channel label must: be at least six characters long, begin with a letter, and contain only lowercase letters, digits, dashes (-), and periods(.). Also enter the URL of the channel's GPG key. Although this field is not required, it is recommended to enhance security. For instructions on generating GPG keys, refer to the *RHN Channel Management Guide*.
5. Click **Create Channel**.

5.2. Uploading Packages

Note

You must be an Organization Administrator to upload packages to private RHN channels. The script will prompt you for your RHN username and password.

After creating the private channel, upload the package headers for the binary and source RPMs to the RHN Server and copy the packages to the RHN Proxy Broker Server. To upload the package headers for the binary RPMs, issue the following command:

```
rhn_package_manager -c "label_of_private_channel" pkg-list
```

This command will upload the header of the package to the channel name specified, and the package itself to **/var/spool/rhn-proxy/rhn**.

pkg-list is the list of packages to be uploaded. Alternatively, use the **-d** option to specify the local directory that contains the packages to add to the channel. Ensure that the directory contains only the packages to be included and no other files. RHN Package Manager can also read the list of packages from standard input (using **--stdin**).

To upload the package headers for the source RPMs:

```
rhn_package_manager -c "label_of_private_channel" --source pkg-list
```

If you have more than one channel specified (using **-c** or **--channel**), the uploaded package headers will be linked to all the channels listed.

Note

If a channel name is not specified, the packages are not added to any channel. The packages can then be added to a channel using the Red Hat Network web interface. The interface can also be used to modify existing private channels.

After uploading the packages, you can immediately check the RHN Web interface to verify their presence. Click **Channels** in the top navigation bar, **Manage Software Channels** in the left navigation bar, and then the name of the custom channel. Then click the **Packages** subtab. Each RPM should be listed.

Also check to see if the local directory is in sync with the RHN Server's image of the channels at the command line:

```
rhn_package_manager -s -c "label_of_private_channel"
```

The **-s** option will list all the missing packages (packages uploaded to the RHN Server not present in the local directory). You must be an Organization Administrator to use this command. The script will prompt you for your RHN username and password.

If you are using the RHN Package Manager to update local packages, you must go to the RHN website to subscribe the system to the private channel.

Chapter 6. Upgrade Installation

This chapter describes how to upgrade your installation of the RHN Proxy Server. It presumes that you have a fully running RHN Proxy Server as well as the required entitlements for it.

6.1. Pre-Requisites

For the latest version of RHN Proxy Server, it requires:

- Red Hat Enterprise Linux 5 (32-bit or 64-bit) or Red Hat Enterprise Linux 6 (64-bit only).
- The deletion of the old Proxy Server's system profile from Red Hat Network Classic or the parent Satellite Server (if applicable).

6.2. Upgrade Installation Process

1. Back up your Proxy Server. If applicable, restore the SSL build direction from the backup to the directory **/root/ssl-build**.
2. Register the Proxy Server to either Red Hat Network Classic or the parent Satellite Server (if applicable) Make sure that the Proxy Server is subscribed to both the Red Hat Enterprise Linux Server base channel and the Red Hat Network Tools child channel.
3. Install the **spacewalk-proxy-installer** package from the Red Hat Network Tools child channel:

```
# yum install spacewalk-proxy-installer
```

4. install the latest version of Proxy, as documented in Section 4.2, “RHN Proxy Server Installation Process”.

Note

If the Proxy server is registered to Red Hat Network Classic and the Proxy Server previously managed custom channels, you will need to restore the custom package repository from the pre-upgrade backup. The permissions and ownership will also need to be set up properly.

```
# chmod 0750 /var/spool/rhn-proxy
# chown apache:apache /var/spool/rhn-proxy
# mkdir -m 0750 -p /var/spool/rhn-proxy/list
# chown apache:apache /var/spool/rhn-proxy/list
```

The default custom package repository is usually **/var/spool/rhn-proxy**.

5. After the installation, update the server to the latest errata updates:

```
# yum update
```

6. Restart the RHN Proxy Server services and test the RHN Proxy Server's functionality:

```
# /usr/sbin/rhn-proxy restart
```

Chapter 7. Troubleshooting

This chapter provides tips for determining the cause of the most common errors associated with RHN Proxy Server and resolving the most common errors associated with it. If you need additional help, contact Red Hat Network support at https://rhn.redhat.com/help/contact.pxt. Log in using a Satellite-entitled account to see a full list of options.

7.1. Managing the Proxy Service

Since the RHN Proxy Server consists of a multitude of individual components, Red Hat provides a script called **rhn-proxy**, that allows administrators to stop, start, restart, or retrieve status on the Proxy.

Table 7.1. rhn-proxy commands

Command	Function
/usr/sbin/rhn-proxy start	This command will start the RHN Proxy Server if it isn't already started.
/usr/sbin/rhn-proxy stop	This command will stop the RHN Proxy Server if it isn't already stopped.
/usr/sbin/rhn-proxy restart	This command will stop the currently running RHN Proxy Server and restart it. If the RHN Proxy Server is stopped, it will simply start it.
/usr/sbin/rhn-proxy status	This command will display the RHN Proxy Server's current status.

7.2. Log Files

Virtually every troubleshooting step should start with a look at the associated log file or files. These files provide invaluable information about the activity that has taken place on the device or within the application and can be used to monitor performance and ensure proper configuration. See Table 7.2, “Log Files” for the paths to all relevant log files:

Table 7.2. Log Files

Component	Log File Location
Apache Web server	**/var/log/httpd/** directory
Squid	**/var/log/squid/** directory
RHN Proxy Broker Server	**/var/log/rhn/rhn_proxy_broker.log**
RHN SSL Redirect Server	**/var/log/rhn/rhn_proxy_redirect.log**
Red Hat Update Agent	**/var/log/yum.log**

7.3. Questions and Answers

This section contains the answers to the most frequently asked questions regarding installing and configuring an RHN Proxy Server solution.

Q: After configuring the RHN Package Manager how can I determine if the local packages were successfully added to the private RHN channel?

A: Use the command **`rhn_package_manager -l -c "name_of_private_channel"`** to list the private channel packages known to the RHN Servers. Or visit the RHN Web interface.

After subscribing a registered system to the private channel, you can also execute the command **`up2date -l --showall`** on the registered system and look for the packages from the private RHN channel.

Q: I've changed the DNS name setting of my Proxy Server, and now my client systems can't update. How can I fix this?

A: Run the **`up2date -u`** command on the client system for the name change to take effect.

Q: How can I determine whether the clients are connecting to the Squid server?

A: The **`/var/log/squid/access.log`** file logs all connections to the Squid server.

Q: The Red Hat Update Agent on the client systems does not connect through the RHN Proxy Server. How can I resolve this error?

A: Make sure that the latest version of the Red Hat Update Agent is installed on the client systems. The latest version contains features necessary to connect through an RHN Proxy Server. The latest version can be obtained through the Red Hat Network by issuing the command **`yum update yum`** as root or from http://www.redhat.com/support/errata/.

The RHN Proxy Server is an extension of Apache. See Table 7.2, “Log Files” for its log file location.

Q: My RHN Proxy Server configuration does not work. Where do I begin troubleshooting it?

A: Make sure **`/etc/sysconfig/rhn/systemid`** is owned by root.apache with the permissions 0640.

Read the log files. A list is available at Table 7.2, “Log Files”.

7.4. General Problems

To begin troubleshooting general problems, examine the log file or files related to the component exhibiting failures. A useful exercise is to **`tail`** all log files and then run **`up2date --list`**. You should then examine all new log entries for potential clues.

A common issue is full disk space. An almost sure sign of this is the appearance of halted writing in the log files. If logging stops during a write, such as mid-word, you likely have filled disks. To confirm this, run this command and check the percentages in the Use% column:

```
df -h
```

In addition to log files, you can obtain valuable information by retrieving the status of your various components. This can be done for the Apache Web server and Squid.

To obtain the status of the Apache Web server, run the command:

```
service httpd status
```

To obtain the status of Squid, run the command:

```
service squid status
```

If the administrator is not getting email from the RHN Proxy Server, confirm the correct email addresses have been set for **traceback_mail** in **/etc/rhn/rhn.conf**.

7.5. Host Not Found/Could Not Determine FQDN

Because RHN configuration files rely exclusively on fully qualified domain names (FQDN), it is imperative that key applications are able to resolve the name of the RHN Proxy Server into an IP address. Red Hat Update Agent, Red Hat Network Registration Client, and the Apache Web server are particularly prone to this problem with the RHN applications issuing errors of "host not found" and the Web server stating "Could not determine the server's fully qualified domain name" upon failing to start.

This problem typically originates from the **/etc/hosts** file. Confirm this by examining the **/etc/nsswitch.conf** file, which defines the methods and the order by which domain names are resolved. Usually, the **/etc/hosts** file is checked first, followed by Network Information Service (NIS) if it is being used, followed by DNS. One of these has to succeed for the Apache Web server to start and the RHN client applications to work.

To resolve this problem, identify the contents of the **/etc/hosts** file. It may look like this:

```
127.0.0.1 this_machine.example.com this_machine localhost.localdomain \
localhost
```

In a text editor, remove the machine host information from the file, it should look like so:

```
127.0.0.1 localhost.localdomain.com localhost
```

Save the file and attempt to re-run the RHN client applications or the Apache Web server. If they still fail, explicitly identify the IP address of the Proxy in the file, such as:

```
127.0.0.1 localhost.localdomain.com localhost
123.45.67.8 this_machine.example.com this_machine
```

Replace the value here with the actual IP address of the Proxy. This should resolve the problem. Keep in mind, if the specific IP address is stipulated, the file will need to be updated when the machine obtains a new address.

7.6. Connection Errors

If you are experiencing problems that you believe to be related to failed connections, follow these measures:

- Confirm the correct package:

  ```
  rhn-org-httpd-ssl-key-pair-MACHINE_NAME-VER-REL.noarch.rpm
  ```

  is installed on the RHN Proxy Server and the corresponding **rhn-org-trusted-ssl-cert-**

`*.noarch.rpm` or raw CA SSL public (client) certificate is installed on all client systems.

- Verify the client systems are configured to use the appropriate certificate.
- If using one or more RHN Proxy Servers, ensure each Proxy's SSL certificate is prepared correctly. If using the RHN Proxy Server in conjunction with an RHN Satellite Server the Proxy should have both its own server SSL key-pair and CA SSL public (client) certificate installed, since it will serve in both capacities. Refer to the SSL Certificates chapter of the *RHN Client Configuration Guide* for specific instructions.
- If the RHN Proxy Server is connecting through an HTTP Proxy, make sure the URL listed is valid. For instance, the HTTP Proxy URL field should not contain references to protocols, such as http:// or https://. Only the hostname and port should be included in the form hostname:port, such as **`your-gateway.example.com:8080`**.
- Make sure client systems are not using firewalls of their own, blocking required ports, as identified in Section 2.4, “Additional Requirements”.

7.7. Caching Issues

If package delivery fails or an object appears to be corrupt, and it is not related to connection errors, you should consider clearing the caches. The RHN Proxy Server has two caches you should be concerned with: one for Squid and the other for authentication.

The Squid cache is located in **`/var/spool/squid/`**. To clear it:

1. Stop the Apache Web server: **`service httpd stop`**
2. Stop the Squid server: **`service squid stop`**
3. Delete the contents of that directory: **`rm -fv /var/cache/rhn/*`**
4. Restart both services:

```
service squid start
service httpd start
```

The same task can be accomplished quicker by just clearing the directory and restarting squid, but this method will most likely result in a number of RHN traceback messages.

The internal caching mechanism used for authentication by the Proxy may also need its cache cleared. To do this, issue the following command:

```
rm -fv /var/cache/rhn/*
```

Although the RHN Authentication Daemon was deprecated with the release of RHN Proxy Server 3.2.2 and replaced with the aforementioned internal authentication caching mechanism, the daemon may still be running on the Proxy. To turn it off, issue the following individual commands in this order:

```
chkconfig --level 2345 rhn_auth_cache off service rhn_auth_cache stop
```

To clear its cache, issue:

```
rm /var/up2date/rhn_auth_cache
```

If the RHN Authentication Daemon has to be retained, which Red Hat recommends against and does not support, note that its performance can suffer from verbose logging. For this reason, its logging (to

/var/log/rhn/rhn_auth_cache.log) is turned off by default. If you do run the daemon and desire logging, turn it back on by adding the following line to the Proxy's **/etc/rhn/rhn.conf** file:

```
auth_cache.debug = 2
```

7.8. Proxy Debugging by Red Hat

If all these troubleshooting steps have been exhausted or if you want to defer them to Red Hat Network professionals, Red Hat recommends that you take advantage of the strong support that comes with RHN Proxy Server.

One way to access that expertise is through the Red Hat Knowledgebase, which provides solutions to the most common issues encountered by users and has a robust browse and search interface for finding the right answers to your Proxy issues. You can access the Red Hat Knowledgebase at http://kbase.redhat.com.

Additionally, Red Hat provides a command line tool called the **SoS Report**, commonly known by its command **sosreport**. This tool collects your Proxy's configuration parameters, log files, and database information and sends it directly to Red Hat.

To use this tool for RHN Satellite Server information, you must have the **sos** package installed. Type **sosreport -o rhn** as root on the Satellite server to create a report. For example:

```
[root@satserver ~]# sosreport -o rhn

sosreport (version 1.7)

This utility will collect some detailed  information about the
hardware and  setup of your  Red Hat Enterprise Linux  system.
The information is collected and an archive is  packaged under
/tmp, which you can send to a support representative.
Red Hat will use this information for diagnostic purposes ONLY
and it will be considered confidential information.

This process may take a while to complete.
No changes will be made to your system.

Press ENTER to continue, or CTRL-C to quit.
```

You are then prompted for your first initial and last name, then a support case number.

It may take several minutes for the system to generate and archive the report to a compressed file. Once finished, email the new file from the **/tmp/** directory to your Red Hat representative for immediate diagnosis.

Sample RHN Proxy Server Configuration File

The **/etc/rhn/rhn.conf** configuration file for the RHN Proxy Server provides a means for administrators to establish key settings. Be warned, however, that errors inserted into this file may cause Proxy failures. Make configuration changes with caution.

If you are also using an RHN Satellite Server, attention to the following parameters are prudent: traceback_mail and proxy.rhn_parent. Review the sample and its comments (beginning with a hash mark #), for additional details.

Note

You may add the **use_ssl** setting to **rhn.conf** for testing purposes only. Set its value to 0 to turn off SSL between the Proxy and the upstream server temporarily. Note though that this greatly compromises security. Return the setting to its default value of 1 to re-enable SSL, or simply remove the line from the configuration file.

```
# Automatically generated RHN Management Proxy Server configuration file.
# ----------------------------------------------------------------------

# SSL CA certificate location
proxy.ca_chain = /usr/share/rhn/RHNS-CA-CERT

# Corporate HTTP proxy, format: corp_gateway.example.com:8080
proxy.http_proxy =

# Password for that corporate HTTP proxy
proxy.http_proxy_password =

# Username for that corporate HTTP proxy
proxy.http_proxy_username =

# Location of locally built, custom packages
proxy.pkg_dir = /var/spool/rhn-proxy

# Hostname of RHN Server or RHN Satellite
proxy.rhn_parent = rhn.redhat.com

# Destination of all tracebacks, etc.
traceback_mail = user0@domain.com, user1@domain.com
```

Revision History

Revision 3-5.400 **2013-10-31** **Rüdiger Landmann**
Rebuild with publican 4.0.0

Revision 3-5 **Wed Sept 19 2012** **Dan Macpherson**
Final packaging for 5.5

Revision 3-4 **Wed Jul 4 2012** **Athene Chan**
Prepared for 5.5 release
Technical review changes incorporated
BZ#491007 Added Chapter on Upgrade Install

Revision 3-0 **Wed Jul 4 2012** **Athene Chan**
Prepared for 5.5 release
Technical review changes incorporated
BZ#491007 Added Chapter on Upgrade Install

Revision 2-5 **Thu Jan 5 2012** **Lana Brindley**
BZ#682996 - Installation chapter - Update instructions
BZ#705755 - Package manager chapter - Additional info
BZ#722193 - Requirements chapter - Fixed error
BZ#729617 - Installation chapter - Fixed error
BZ#729663 - Installation chapter - Added admonition

Revision 2-4 **Mon Aug 15 2011** **Lana Brindley**
Folded z-stream release into y-stream

Revision 2-3 **Wed Jun 22 2011** **Lana Brindley**
BZ#713527 - Added RHEL 6 references

Revision 2-2 **Wed Jun 15 2011** **Lana Brindley**
Prepared for publication

Revision 2-1 **Fri May 27 2011** **Lana Brindley**
Updates from translators

Revision 2-0 **Fri May 6 2011** **Lana Brindley**
Prepared for translation

Revision 1-9 **Wed April 27 2011** **Lana Brindley**
BZ#653844 - QE Review

Revision 1-8 **Mon Feb 7 2011** **Lana Brindley**
BZ#646176 - Installation

Index

A

additional requirements, Additional Requirements

advantages, RHN Proxy Server

authentication, How Proxy Works

authentication caching
- clearing, Caching Issues

C

caching issues, Caching Issues

channel, Frequently Used Terminologies
- creating a private channel, Creating a Private Channel

Channel Adminstrator, Frequently Used Terminologies

client configuration
- subscribe to private channel, Uploading Packages

connection errors, Connection Errors

D

disk space requirements, Disk Space Requirements

F

Frequently Used Terminologies, Frequently Used Terminologies

G

general problems, General Problems

H

hardware requirements, Hardware Requirements

host not found error
- could not determine FQDN, Host Not Found/Could Not Determine FQDN

how proxy works, How Proxy Works

HTTP Proxy Caching Server
- disk space requirements, Disk Space Requirements

I

inbound ports, satellite
- 5222, Additional Requirements

installation

- base, Base Install
- of RHN Proxy Server, RHN Proxy Server Installation Process

L

log files, Log Files

O

Organization Administrator, Frequently Used Terminologies

outbound ports
- 80, 443, Additional Requirements

P

port
- 443, Additional Requirements
- 5222, Additional Requirements
- 80, Additional Requirements

port 443, Additional Requirements

port 4545, Additional Requirements

port 80, Additional Requirements

private channel, Creating a Private Channel

Proxy Ports, Additional Requirements

Q

questions and answers, Questions and Answers

R

Red Hat Network
- introduction, Red Hat Network

Red Hat Update Agent, Frequently Used Terminologies, How Proxy Works

requirements, Requirements
- additional, Additional Requirements
- disk space, Disk Space Requirements
- hardware, Hardware Requirements
- software, Software Requirements

RHN Authentication Daemon, disabling
- rhn_auth_cache, stopping, Caching Issues

RHN Package Manager, How Proxy Works, RHN Package Manager and Serving Local

Packages
- channels, specifying, Uploading Packages
- command line options, RHN Package Manager and Serving Local Packages
- configuration file, RHN Package Manager and Serving Local Packages
- configuring, Creating a Private Channel
- create private channel, Creating a Private Channel
- installing, RHN Package Manager and Serving Local Packages
- upload package headers, Uploading Packages
- verify local package list, Uploading Packages

rhn-proxy
- service, Managing the Proxy Service

rhn.conf
- sample file, Sample RHN Proxy Server Configuration File

rhn_package_manager , Uploading Packages (see RHN Package Manager)

S

satellite-debug, Proxy Debugging by Red Hat

software requirements, Software Requirements

squid caching, Caching Issues

T

topologies, Example Topologies
- multiple proxies horizontally tiered, Multiple Proxy Horizontally Tiered Topology
- multiple proxies vertically tiered, Multiple Proxy Vertically Tiered Topology
- proxies with RHN Satellite Server, Proxies with RHN Satellite Server
- single proxy, Single Proxy Topology

traceback, Frequently Used Terminologies

troubleshooting, Troubleshooting